OPINIÓN

El hackeo de Guacamaya y el hacktivismo de bandera falsa

Por Ernesto Ángeles · 5 de octubre de 2022 · 7 min de lectura

El pasado jueves 29 de septiembre el comunicador preferido de la derecha mexicana, Loret de Mola, dio a conocer información sensible que le fue entregada como resultado de un hackeo masivo a la Sedena, en donde entre otras cosas, se dio a conocer el estado de salud del presidente López Obrador; esto generó una avalancha de movimiento digital que fue creciendo conforme se añadían nuevas declaraciones y pronunciamientos al respecto, desde la respuesta del presidente en "la mañanera", hasta la creación de un perfil en Twitter de los supuestos atacantes cibernéticos, los cuales se hacen llamar "Guacamaya" y se identifican como un grupo "hacktivista".

Antes de entrar en detalles como la falsedad del perfil de Twitter creado por el supuesto grupo, la poca coherencia político-ideológica que ha exhibido su perfil o el fuerte parecido que existe entre esta estrategia y la supuesta declaración de guerra que le hizo una cuenta falsa (y mal hecha) de Anonymous al gobierno del presidente López Obrador tiempo atrás; es necesario señalar cuestiones básicas en la cultura hacker y el activismo digital, tal como qué es el hacktivismo, su relación histórica con los "whistleblowers" y la propia historia de Anonymous, ya que existen gran cantidad de inexactitudes y confusiones (naturales e inducidas) de las que la oposición ha echado mano, al punto de comparar a personajes bastante nefastos y mal intencionados como Loret o Peniley con Julian Assange, aún cuando sus métodos y motivaciones sean radicalmente opuestos.

El hacktivismo, tal como su nombre lo dice, es la unión entre las prácticas de hackeo y el activismo político, más exactamente, el hacktivismo puede comprenderse como el uso políticamente motivado de habilidades de hackeo realizadas por actores no gubernamentales anónimos con el fin de promover un tema y una visión, llamar la atención sobre un problema y, últimamente, provocar un cambio en la sociedad.

El grupo hacktivista más conocido a nivel mundial es Anonymous, el cual nació en 2003 en un foro de 4Chan, entre sus motivaciones iniciales estaba un activismo dirigido especialmente al ciber idealismo y su negativa de permitir que se implementaran controles de copyright porque iban en contra de la naturaleza de internet; sin embargo, conforme se sucedieron eventos como el ataque jurídico-institucional estadounidense contra Wikileaks (una página que nació como el esfuerzo de whistleblowers), las primaveras árabes o el exitoso reclutamiento digital de ISIS; los objetivos de Anonymous se diversificaron. Sin embargo, la presencia y operaciones digitales de Anonymous comenzaron a reducirse drásticamente a partir de 2015 y principios de 2016, cuando algunos de sus miembros más activos y centrales comenzaron a ser perseguidos y encarcelados a nivel mundial.

Y es que, contraria a la extendida creencia que Anonymous era un movimiento distribuido, horizontal y masivo, el grupo contaba con personajes clave (con los conocimientos y habilidades para hackear) mientras que muchos de los voluntarios sólo accionaban programas dirigidos para atacar redes o, más aún, los personajes centrales contaban con redes de computadoras "zombis", dispositivos infectados con programas para lanzar ataques sin que sus dueños lo supieran siquiera.

Por otro lado, un whistleblower es una persona que revela información interna de una organización (ya sea pública o privada), dicha información a menudo revela un comportamiento ilegal, ilícito, inmoral, riesgoso o fraudulento de las organizaciones; por tanto, las motivaciones de los whistleblowers pueden ser morales, personales, sociales, políticas o cualquier otra que los conmine a revelar información, ya sea al público en general o al interior de las propias organizaciones; entre los casos más conocidos de whistleblowers están: Julian Assange, Edward Snowden, Chelsea Manning o Chistopher Wylie.

Históricamente, existen numerosos ejemplos de cooperación entre comunidades hacktivistas y whistleblowers, con Anonymous y Wikileaks como el primer lugar; así como también existen casos en donde los métodos y las motivaciones de ambas figuras se mezclan; sin embargo, dada la versatilidad de internet y la dificultad de atribución de atacantes, también existen casos denominados "de bandera falsa", en donde un grupo o actor se hacen pasar por hactivistas para filtrar información con evidentes motivaciones políticas, tal como sucedió en las elecciones presidenciales en 2016 en Estados Unidos, cuando un grupo (supuestamente a cargo de los servicios de inteligencia de Rusia) hackeó los servidores de correo de los demócratas y filtró la información en Wikileaks, dañando en el proceso la campaña de la entonces candidata, Hillary Clinton.

En el caso de operaciones de bandera falsa, el hacktivismo resulta bastante atractivo, ya que cuenta con legitimidad por sí mismo gracias a la mercadotecnia de la cultura pop y a una buena dosis de idealismo (y promoción) cibernética, lo que le ha brindado a la leyenda de Anonymos (y al hacktivismo) una confianza de la que pocos medios de comunicación e información tienen a nivel mundial, lo que ha generado que este tipo de ataques sean cada vez más usados https://www.verdict.co.uk/false-flag-hacktivism/

Además, en algún momento las fronteras entre hacktivismo y actividad maliciosa realizada por un Estado o agencia de inteligencia se entrecruzan, al punto de establecerse relaciones mutuamente benéficas, con casos paradigmáticos como el de los "hackers patrióticos", los cuales llevan a cabo operaciones cibernéticas que sirven al interés de sus países pero bajo el cobijo de ser ciudadanos, tal como ha sucedido con hackers rusos, estadounidenses o chinos.

Por si fuera poco, también es posible que un actor que pertenece a alguna agencia de inteligencia o aparato militar se haga pasar como parte de un grupo de hacktivistas, ya que esta clase de grupos no requieren de una autenticación de usuario o de identidad real, sino que sólo es necesario sumarse en algún foro o grupo en internet, lo que vuelve aún más turbio la posible implicación de actores mal intencionados en las operaciones de hacktivistas, en donde las habilidades y conocimientos técnicos juegan un papel medular.

Una vez mencionado lo anterior, resulta interesante analizar el discurso, intereses y actuación del supuesto grupo hacktivista Guacamaya, ya que se auto denominan en contra del imperialismo y el expolio; sin embargo, sus objetivos únicamente son países gobernados por la izquierda: Perú, Chile, Colombia y México, sin siquiera fijarse en Estados Unidos o Canadá, los países que realmente ejercen el poder. Por otro lado, resulta interesante que los principales objetivos de Guacamaya hayan sido instituciones militares y de seguridad, ya que salta la pregunta ¿realmente su ciberseguridad es tan deficiente en todos estos países o es que los atacantes contaban con conocimientos técnicos e institucionales suficientes?

Otra de las preguntas que saltan a la vista es la motivación y los conocimientos requeridos para llevar a cabo la operación, ya que las redes militares no es que se encuentren tan fácilmente como googlear: ¿Dónde están los puntos de acceso a las redes de Sedena o el ejército de Chile? A su vez, no sólo es necesario saber cómo acceder, sino que implica una serie de pasos tal como dónde, qué, para qué y con qué, en donde no sólo es necesaria la pericia técnica, sino un conocimiento más a fondo de los objetivos.

En resumen: ¿En realidad las redes militares de países como México, Perú, Colombia, Guatemala o Chile son tan poco seguras que cualquier hacktivista puede acceder? En tal caso, ¿Cómo fue el proceso de ponderación de objetivos y por qué justamente esos? Dado que la motivación política de Guacamaya, más allá del discurso idealista

y engrandecedor, es bastante clara y está dirigida en contra de gobiernos de izquierda y sus aparatos de seguridad (mismos que se nos olvida que son fundamentales para garantizar la gobernabilidad de cualquier país frente a amenazas internas… y externas).

Y en el caso de México ¿Por qué un grupo con convicciones tan cercanas a la izquierda le daría esta información a uno de los principales voceros de la derecha? ¿Por qué existe una cuenta de Twitter de Guacamaya si el propio colectivo anunció que no tendrían redes sociales? ¿Por qué tal cuenta de Twitter primero se pronunció anti comunista y anti socialista y en otro momento se dijo a favor de salvar el planeta? ¿Cuál es su interés con la Sedena y su motivación para alimentar a los voceros de derecha en un momento en donde, casualmente, está en pleno el debate sobre la permanencia del ejército en labores de seguridad pública? ¿Por qué un grupo tan motivado por el ambientalismo no se lanza en contra de las mega contaminantes mineras canadienses o las transnacionales estadounidenses?

Publicado en Punto de Referencia. Dirección original: https://puntodereferencia.mx/opinion/el-hackeo-de-guacamaya-y-el-hacktivismo-de-bandera-falsa
Descargado el 21 de noviembre de 2026.